International Journal of LNCT, Vol 2(4)
ISSN (Online): 2456-9895

A novel LSB based multi-level encryption image steganography:a review

Ganga Verma[1] and Vikram Rajpoot[2]
Research Scholar, Department of Computer Science, LNCT, Bhopal[1]
Assistant Professor, Department of Computer Science, LNCT, Bhopal[2]

Abstract

In today's world there is a lot of advancement in technology especially in communication which is leading us to live a happy life and on the other side it is also leading us to live an insecure life due to exploitation of advanced technology in communication. Now exploitation has become the major criteria which should be solved. To solve this issue various techniques such as Cryptography, Watermarking, Steganography and some other different techniques have been developed. The main goal of using the steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this goal that has been planned to achieve the security of the secret messages, because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message. Steganography is the art and science of hiding important information in such a way that only the specific person can retrieve the hidden information. These review research highlighted on LSB based Steganography techniques.

Keywords

Steganography, LSB, Multi-level encryption, Image steganography.

1.Introduction

The word steganography is derived from the Greek words stegos meaning cover and grafia meaning writing [1] defining it as covered writing. In image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication. Constantly communicated through the Internet are flows of information generated from many diverse applications such as e-commerce transactions, audio and video streaming or online chatting. The security of such data communication, which is required and vital for many applications nowadays, has been a major concern and ongoing topic of study given that the Internet is by design open and public in nature. Many techniques have been proposed for providing a secure transmission of data. Data encryption and information hiding techniques have become popular and generally complement each other. Whereas encryption transforms data into seemingly meaningless bits, called ciphertext, through the use of sophisticated and robust algorithm, information hiding [1] is the process of concealing messages in such a way that no one apart from the sender and the intended receiver even knows that there is a hidden message. The word steganography is of Greek origin which means "covered or hidden writing" [2]. The technique has been used in ancient times where secret messages were tattooed on the shaven heads of the messengers. These messengers were sent away after their hair grew up and were later shaved again to recover the messages.

The general idea of hiding secret information in media has a wider range of applications that go beyond steganography. For example, an image printed on a document could be annotated by metadata that could lead a user to its higher resolution. Due to the high proliferation of digital images and the high degree of redundancy present in digital images, there is an increased interest in the usage of images as the cover object in steganography. The Least-Significant-Bit (LSB) technique is one of the most widely used scheme for image steganography. This technique involves the modification of the LSB planes of the images. In this technique, the message is stored in the LSB of the pixels which could be considered as random noise.

Therefore altering them does not significantly affect the quality of the cover image. Variations of the LSB algorithms include one or more LSB bits. The motivation for this study is to provide security to confidential RGB images such as maps or sensitive signed documents. The basic principle of steganography is to hide the secret information in the cover object, which can be a digital medium such as image, audio or video file, to obtain a stego file that has secret information hidden in it. In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e image, video, audio, text) and select the effective secret messages as well as the robust password (which supposed to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or

chatting, or by other modern techniques. The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password used by the sender. The Steganography system scenario is shown above in the Figure 1.

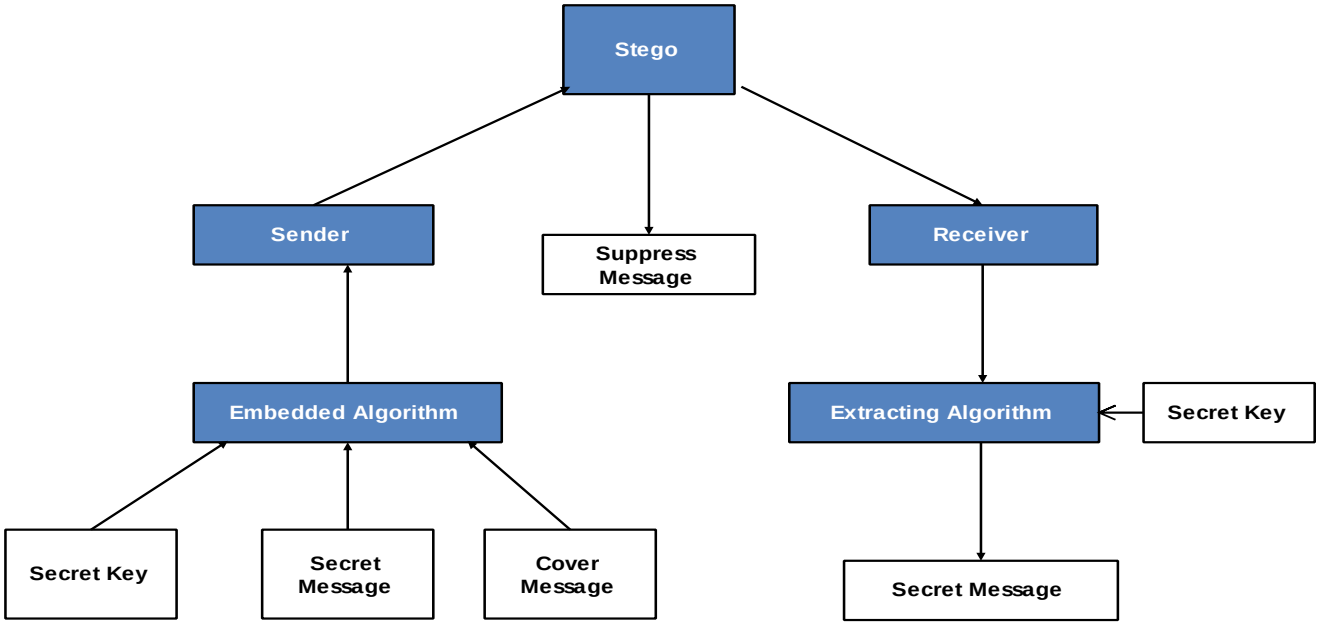

Figure 1 Steganography system scenarios [10]

2.Data hiding techniques

Steganography techniques aimed at secretly hiding data in a multimedia carrier such as text, audio, image or video, without raising any suspiscion of alteration to its contents. The original carrier is referred to as the cover object.

A. Injection

The data can be hidden in sections of a file that are ignored by the processing application using injection technique. Therefore file bits that are relevant to an end-user are not modified leaving the cover file perfectly usable. For example, we can add additional harmless bytes in an executable or binary file. Because those bytes don't affect the process, the end-user may not even realize that the file contains additional hidden information. However, using an insertion technique changes file size according to the amount of data hidden and therefore, if the file looks unusually large, it may arouse suspicion.

B. Substitution

Substitution technique is used to replace the least significant bits of information that determine the meaningful content of the original file with new data in a way that causes the least amount of distortion. The main advantage of this technique is that the cover file size does not change after the execution of the algorithm. On the other hand, this approach has at least two drawbacks. First, the resulting stego object may be adversely affected by quality degradation—and that may arouse suspicion. Second, substitution limits the amount of data that you can hide to the number of insignificant bits in the file.

C. Generation

Unlike injection and substitution, generation techniques do not require an existing cover file. This technique generates a cover file for the sole purpose of hiding the message. The main flaw of the insertion and substitution techniques is that people can compare the stego object with any pre-existing copy of the cover object (which is supposed to be the same object) and discover differences between the two. We will not have that problem when using a generation approach, because the result is an original file.

3.Previous work

G. S. Charan, Nithin Kumar S S V, Karthikeyan B, Vaithiyanathan V and Divya Lakshmi K,[1] Steganography is an art of hiding the existence of secret information by embedding it in a cover and hence preventing the unauthorized access of confidential information. Presented a novel approach

of encrypting the plain text into cipher text and embedding it into a color image. Encryption is done in two stages, during first stage it is encrypted by Ceaser cipher technique and in the second stage it is encrypted based on chaos theory. The cipher text obtained after encryption is embedded using 3, 3, 2 LSB replacement algorithm.

S. Islam and P. Gupta,[2] a novel steganography technique to embed secret message in a grayscale image has been proposed. Pixels belonging to edges of the cover image are used as the embedding locations. The edge selection approach is data adaptive that means, numbers of pixels belonging to edges are selected on the basis of payload to be embedded. The embedding approach is designed to provide better security. Experimental results demonstrate that the proposed technique outperforms the existing practical state-of-the-art techniques and at par with simulated version of minimizing distortion based approach.

M. M. Sadek, M. G. M. Mostafa and A. S. Khalifa,[3] Recently, information hiding in human skin regions has improved robustness of image steganography and yield better imperceptibility. Present a skin-tone block-map algorithm for hiding data in colored images. A skin-tone map is generated from the host image using a skin-tone detection algorithm that is based on the pixel color information. The skin-tone map is then converted to a skin-tone block-map, which is used for hiding the secret data. Moreover, the embedding process is carried out in the wavelet domain and the extraction is carried out blindly. Experimental results and comparisons with related work show the efficiency of the proposed method and its resistance to attacks such as JPEG compression.

A. K. Bairagi, S. Mondal and R. Debnath,[4] A RGB channel based steganographic technique for images imparting better information security. This technique inserts the information into deeper layers of the selected RGB channel and the position is determined depending on the status of channel and value of the secret key. Pixels of the cover image are selected depending on the environment of the channels and hidden information. The ambiguity of pixel, channel and position selection process increases robustness of the steganographic system. The technique is also less vulnerable to unintentional attacks like image manipulation as data hides in the deeper layer of the pixels. The system uses the RGB channels of the stego-image and the secret key to extract the hidden information. The use of secret key gives another way to secure the information from malicious user. The experiment shows that on average 77.00% pixels of the cover image are used for hiding secret information and produces high PSNR value which indicates the capacity and imperceptibility of the technique respectively.

R. Kumar and S. Chand,[5] A new image steganography scheme for colored images based on the cluster analysis. In this scheme, analyze the secret data in order to make its clusters. The secret data can be textual, image/video or audio/speech. A cluster contains ASCII values of characters if the secret data is text, sample values for audio/speech and pixel values in case it is image/video. We then calculate the difference value between the secret data and the minimum value contained in the cluster. We do not hide actual secret data; the difference value is embedded equally into two channels of the image. The experimental results show that our proposed method has enhanced security as compared to the modified Kekre algorithm and pixel intensity based high capacity data embedding method [9]. Furthermore, our scheme has good hiding capacity, high PSNR value, and very low MSE value.

H. Hajizadeh, A. Ayatollahi and S. Mirzakuchaki,[6] A new high capacity method for spatial domain image steganography is introduced. The proposed block-based and high capacity steganographic method is the extended form of Zhang and Wang's EMD method and uses eight modification directions to hide multiple secret bits into a cover pixel pair at a time. The proposed algorithm has been optimized to select blocks of the image in a random order scheme, to eliminate the bias between the image and the confidential data. The suggested method has also been combined with the Yang's Inverted Pattern (IP) approach and personally defined XORed pattern (XORP) and XNORed pattern (XNORP) approaches to achieve further enhancement. Simulation results shows that the proposed method can obtain various hiding capacities of 1 to 5 bpp and corresponding good visual qualities of either 53.68 to 30.05 dB or 52.97 to 29.40 dB in the case of 4×4 or 8×8 blocks, respectively. The experimental results show that our proposed method has better results in terms of both data embedding capacity and visual quality than that of previous works.

4.Problem statement

In modern age of information technology unauthorized access of information increasing day by day due to this secure information needed and this can be done using cryptography or steganography technique[7-9]. There are many image steganography and cryptography algorithms has been already developed such as Least Significant Bit (LSB), Random Scattered (RS), Most Significant Bit (MSB) but LSB is most frequently used because it simply inserts the bit of secret message with the least significant bit of image. LSB is very simple due to this detection of secret message is also easy, therefore a high secure improved version of LSB algorithms is need to develop which is more secure than LSB[10-12].

5. Conclusion

In this research our concern in image stenography because of it's widely used in Internet and also in mobile system. Improved LSB algorithm can easily be implemented and do not visually degrade the image to the point of being noticeable. It would appear that Improved LSB is good algorithm of Steganography due to its security. Using Improved LSB algorithm can exchange secret messages over public channel in a safe way. Image steganography is broadly used in steganography field. So there is lot to do as per research is concerned. With continued research and improvement in algorithm design, steganography can be taken as a serious means to hide data and the present work appears that it was more efficient in hiding more data (payload) than the algorithm used in S- Tools [9].

References

[1] Charan GS, SSV NK, Karthikeyan B, Vaithiyanathan V. A novel LSB based image steganography with multi-level encryption. In innovations in information, embedded and communication systems (ICIIECS), International conference on 2015 (pp. 1-5). IEEE.

[2] Islam S, Gupta P. Robust edge based image steganography through pixel intensity adjustment. In high performance computing and communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl conferences on embedded software and system (HPCC, CSS, ICESS), 2014 IEEE international conferences on 2014 (pp. 771-7). IEEE.

[3] Sadek MM, Mostafa MG, Khalifa AS. A skin-tone block-map algorithm for efficient image steganography. In informatics and systems (INFOS), 2014 9th international conference on 2014 (pp. DEKM-27). IEEE.

[4] Bairagi AK, Mondal S, Debnath R. A robust RGB channel based image steganography technique using a secret key. In computer and information technology (ICCIT), 2013 16th International conference on 2014 (pp. 81-7). IEEE.

[5] Kumar R, Chand S. A new image steganography technique based on similarity in secret message. 2013.

[6] Hajizadeh H, Ayatollahi A, Mirzakuchaki S. A new high capacity and EMD-based image steganography scheme in spatial domain. In electrical engineering (ICEE), 2013 21st iranian conference on 2013 (pp. 1-6). IEEE.

[7] Singla D, Juneja M. New information hiding technique using features of image. Journal of Emerging Technologies in Web Intelligence. 2014; 6(2):237-42.

[8] Mainberger M, Schmaltz C, Berg M, Weickert J, Backes M. Diffusion-based image compression in steganography. In international symposium on visual computing 2012 (pp. 219-28). Springer, Berlin, Heidelberg.

[9] Budhia U, Kundur D. Digital video steganalysis exploiting collusion sensitivity. In sensors, and command, control, communications, and intelligence (C3I) technologies for homeland security and homeland defense III 2004 (pp. 210-22). International Society for Optics and Photonics.

[10] Provos N, Honeyman P. Hide and seek: an introduction to steganography. IEEE Security & Privacy. 2003; 99(3):32-44.

[11] Gomathymeenakshi M, Sruti S, Karthikeyan B, Nayana M. An efficient arithmetic coding data compression with steganography. In emerging trends in computing, communication and nanotechnology (ICE-CCN), International conference on 2013 (pp. 342-5). IEEE.

[12] Lin YK. A data hiding scheme based upon DCT coefficient modification. Computer Standards & Interfaces. 2014; 36(5):855-62.